Systematic cyber attacks against Israeli and Palestinian targets going on for a year

By Snorre Fagerland
Principal Security Researcher

NORMAN®

Summary

We have observed multiple probable malware attacks against Israeli and Palestinian targets. These attacks are likely performed by the same attacker, as the malware in question communicate with the same command- and control structures, and in many cases are signed using the same digital certificate.

These attacks have been ongoing for at least a year; seemingly first focused on Palestinians, then Israelis. The attacker is unknown at this point, but the purpose is assumed to be espionage/surveillance.

Introduction

Recently, media (1) reported of a targeted attack against the Israeli government, in the form of emails purporting to come from IDF Chief of Staff Benny Gantz with a malicious attachment.

IDF strikes militants in Gaza Strip following rocket barrage

The Israeli Air Force carried out a strike on targets in the northern Gaza Strip on Tuesday, after eight mortar shells were fired into southern Israel several hours earlier.

This was an interesting development – Israel has, as far as we know, not been very targeted by spear phishing attacks like this.

In the following text we will usually be referring to the actual malware files we uncovered by their MD5 hash, which is a number that uniquely (well, uniquely enough) identifies the file in question.

The initial reported malware

While we don't have visibility into Israeli government mails, we do receive a lot of suspicious executable files, and a little digging gives results. We found one file which matched the reports:

"IDF strikes militants in Gaza Strip following rocket barrage.doc----------.scr".

This is an executable file, but the icon looks like a document icon, and the very long name makes the *.scr extension hard to spot - particularly if the executable comes packaged in an archive, as was reportedly the case here.

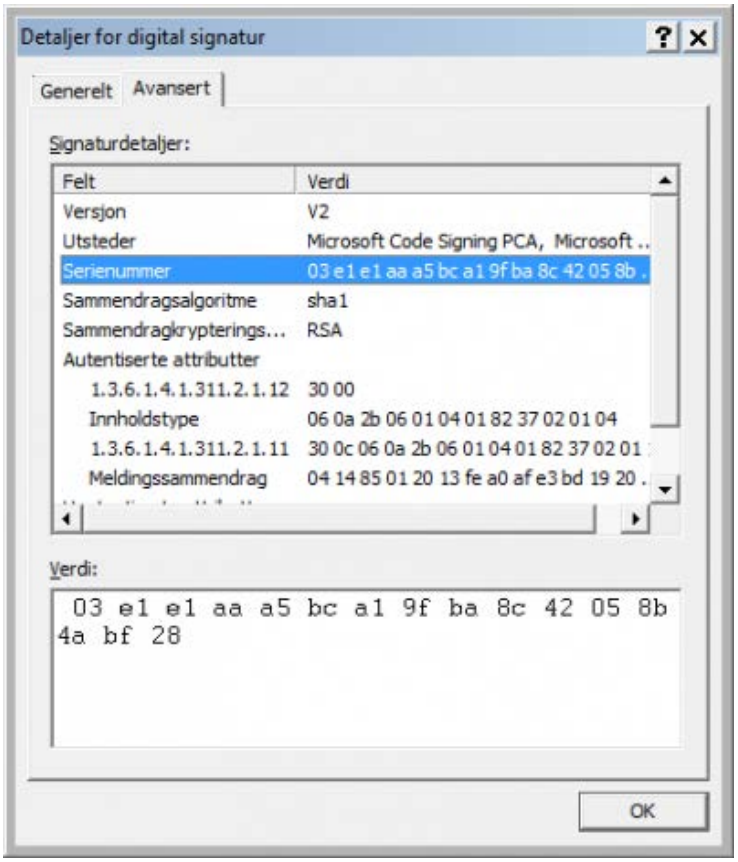
This executable itself is a WinRAR selfextracting (SFX) archive, which contains several other files:

- *Word.exe, an XtremeRat backdoor executable*
- *2.ico, an icon file*
- *barrage.doc, an innocent document containing pictures (above)*

XtremeRat is a commercially available backdoor trojan which has been used in many attacks, targeted and otherwise, over the years. It gained some notoriety in connection with attacks against Syrian activists; along with other off-the-shelf trojans such as BlackShades and DarkComet.

The digital signature

An interesting feature of this exact XtremeRat is that it is digitally signed – seemingly by Microsoft:



The certificate chain ends in an untrusted (faked) root certificate; so it will not validate properly. Nevertheless the certificate is useful for us, as it can be used to find related cases. All certificates are issued with a serial number which normally is quite unique, as it is supposed to be an identifier within the scope of its issuer. So, querying our databases for this particular faked certificate returns a number of files which are probably the products of our Israel-hostile attacker.

SerialNr	Subject	Program	Issuer	MoreInfo	Validates	Times Seen
03E1E1AAA5BCA19FBABC42058B4ABF28	Microsoft Corporation		Microsoft Code Signing PCA		CERT_E_UNTRUSTEDROOT	28
03E1E1AAA5BCA19FBABC42058B4ABF28	Microsoft Corporation	Microsoft Word	Microsoft Code Signing PCA	http://www.Microsoft.com	CERT_E_UNTRUSTEDROOT	1

These files were received in intervals through the fall and summer, going back to May 2012, and reveal more hints about targets. Several of them are self extracting archives containing extra files, such as documents, links and even video. The following pages display some of the bait information the new files contain.

IDF Roundup – What Happened In July 2012

July 2012 was a difficult month for the Israeli people. A terror attack on a bus in Burgas, Bulgaria, killed five Israelis and the Bulgarian driver, and injured dozens more. This month also marked the daring rescue operation at Entebbe in 1976, as well as the prisoner exchange in which the bodies of IDF soldiers Sergeants First Class Ehud Goldwasser and Eldad Regev were returned by Hezbollah.

During July, 22 rockets fired from Gaza hit southern Israel.

Damaged buses at Bulgaria's Burgas airport on Wednesday. Credit: New York Times

July 4: 36th anniversary of Operation Entebbe – An Interview With the Chief Pilot

This July marked the 36th anniversary of Operation Entebbe — a military operation in which the IDF rescued the Israeli hostages who were aboard a hijacked plane that was flown to Entebbe, Uganda, in 1976. Read the full interview with the chief pilot of the operation, Brig. Gen. (res.) Joshua Shani.

Word document, contained in SFX RAR file 66DDF27517985A75B2317231B46A6F62

Secret and exclusive

Hamas will buy rockets from Iran after several days

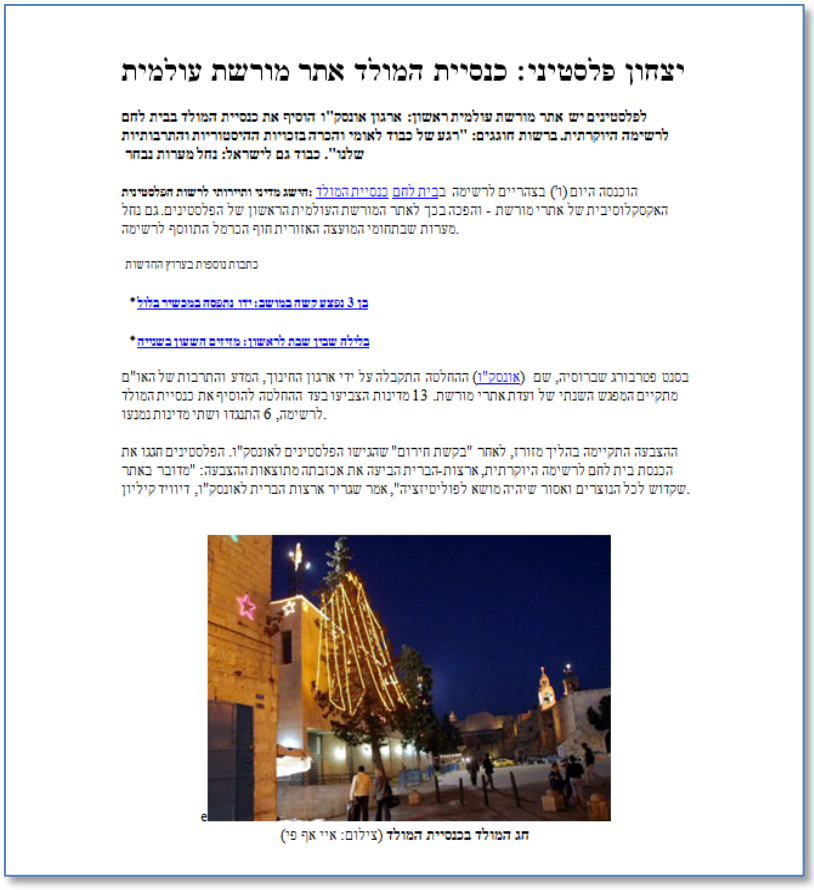
15-5-2012

Qassam

Production of the shorter range Qassam rocket began in September 2001, following the outbreak of the Al-Aqsa Intifada. The rockets have been manufactured and deployed primarily from the Gaza Strip although Israeli Defense Forces have seized rockets in the West Bank. The Qassam rocket is cylindrical and contains a small warhead on its tip. The rocket contains four small stabilizing wings on one end, a middle section containing the engine, and an attached warhead with a detonating fuse on the other end. The rocket is constructed from iron approximately 2.5-3mm thick.

Word document, contained in SFX RAR file 4A06D9989A8C3A9967C2011E5BAF3010

"Report.doc.....
.....
.....exe"



יצחון פלסטיני: כנסיית המולד אתר מורשת עולמית

לפלסטינים יש אתר מורשת עולמית ראשון: ארגון אונסק"ו הוסיף את כנסיית המולד בבית לחם לרשימה היוקרתית. ברשות חוגגים: "רגע של כבוד לאומי והכרה בזכויות ההיסטוריות והתרבותיות שלנו". כבוד גם לישראל: נחל מערות נבחר

חדשות מדיני והזירותי לרשות הפלסטינית: הוכנסה היום (ו') בצהריים לרשימה בבית לחם כנסיית המולד האקסקלוסיבית של אתרי מורשת - והפכה בכך לאתר המורשת העולמית הראשון של הפלסטינים.גם נחל מערות שבתחומי המועצה האזורית חוף הכרמל התווסף לרשימה.

כתבות נוספות בערוץ החדשות

* בן 3 נפצע קשה במושב; ידו נתפסה במכשיר כלול
* בלילה שבין שבת לראשון: מזרם הששון בשנירה

בסנט פטרבורג שברוסיה, שם (אונסק"ו) ההחלטה התקבלה על ידי ארגון החינוך, המדע והתרבות של האו"ם מתקיים המפגש השנתי של ועדת אתרי מורשת. 13 מדינות הצביעו בעד ההחלטה להוסיף את כנסיית המולד לרשימה, 6 התנגדו ושתי מדינות נמנעו.

ההצבעה התקיימה בהליך מזורז, לאחר "בקשת חירום" שהגישו הפלסטינים לאונסק"ו. הפלסטינים חגגו את הכנסת בית לחם לרשימה היוקרתית, ארצות-הברית הביעה את אכזבתה מתוצאות ההצבעה: "מדובר באתר שקדוש לכל הנוצרים ואסור שיהיה מושא לפוליטיזציה", אמר שגריר ארצות הברית לאונסק"ו, דיוויד קיליון.

חג המולד בכנסיית המולד (צילום: איי אף פי)

Word document, contained in SFX RAR file 15FC009D9CAAA8F11D6C3DA2B69EA06E

"Silence of the Jews make the Church of the Nativity of the Palestinians.doc----------.scr"

Found in Israel

IDF NEWS

Israeli Defense and Security Exhibition

http://www.israelpictures.org/?p=1264

Top of Form

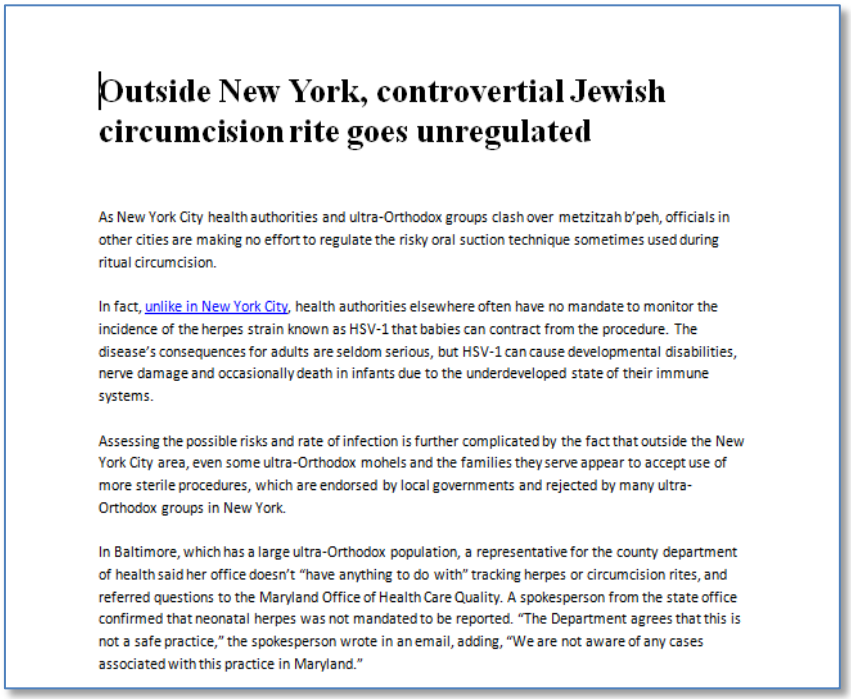
Word document, contained in SFX RAR file 940B3ACDF1E26FCCCF74A5A0359FB079

"IDF NEWS[RTLO]cod.SCR"

3gp video, contained in SFX RAR file
9C39D6F52E1E1BE5AE61BAB90971D054

"A Rood Awakening! Michael Rood .3gp----------.scr"

Found in Israel



Outside New York, controvertial Jewish circumcision rite goes unregulated

As New York City health authorities and ultra-Orthodox groups clash over metzitzah b'peh, officials in other cities are making no effort to regulate the risky oral suction technique sometimes used during ritual circumcision.

In fact, unlike in New York City, health authorities elsewhere often have no mandate to monitor the incidence of the herpes strain known as HSV-1 that babies can contract from the procedure. The disease's consequences for adults are seldom serious, but HSV-1 can cause developmental disabilities, nerve damage and occasionally death in infants due to the underdeveloped state of their immune systems.

Assessing the possible risks and rate of infection is further complicated by the fact that outside the New York City area, even some ultra-Orthodox mohels and the families they serve appear to accept use of more sterile procedures, which are endorsed by local governments and rejected by many ultra-Orthodox groups in New York.

In Baltimore, which has a large ultra-Orthodox population, a representative for the county department of health said her office doesn't "have anything to do with" tracking herpes or circumcision rites, and referred questions to the Maryland Office of Health Care Quality. A spokesperson from the state office confirmed that neonatal herpes was not mandated to be reported. "The Department agrees that this is not a safe practice," the spokesperson wrote in an email, adding, "We are not aware of any cases associated with this practice in Maryland."

Word document, contained in SFX RAR file
9D144A828F757A90B86976EF0C906B3F

Israel upgrades missile defense system

JERUSALEM—An Israeli Defense Ministry official confirms the country has upgraded its top-tier Arrow II missile defense system, as it girds for possible attacks from Iran and Syria.

The official confirmed Sunday that sensors, command and control equipment and radar have been enhanced to improve reach and accuracy. He did not elaborate and spoke on condition of anonymity because he was not authorized to discuss military preparations.

Israel has developed a network of air defense systems to parry an array of threats, including the Arrow, a joint project with the U.S. designed to shoot down incoming missiles launched as far away as Iran.

Israel regards Iran as its main enemy, and suspects Tehran is building nuclear weapons despite its denials.

Israel is also worried about a chemical weapons attack from Syria.

Word document, contained in SFX RAR file
D14E0A3D408065B1551F2827B50B83CA

Advisor: Romney would back Israeli strike on Iran

JERUSALEM (AP) – Mitt Romney would back an Israeli military strike against Iran aimed at preventing Tehran from obtaining nuclear capability, a top foreign policy adviser said early Sunday, outlining the aggressive posture the Republican presidential candidate will take toward Iran in a speech in Israel later in the day.

By Charles Dharapak, AP

Mitt Romney meets Sunday with Israel's Prime Minister Benjamin Netanyahu in Jerusalem.

Enlarge

By Charles Dharapak, AP

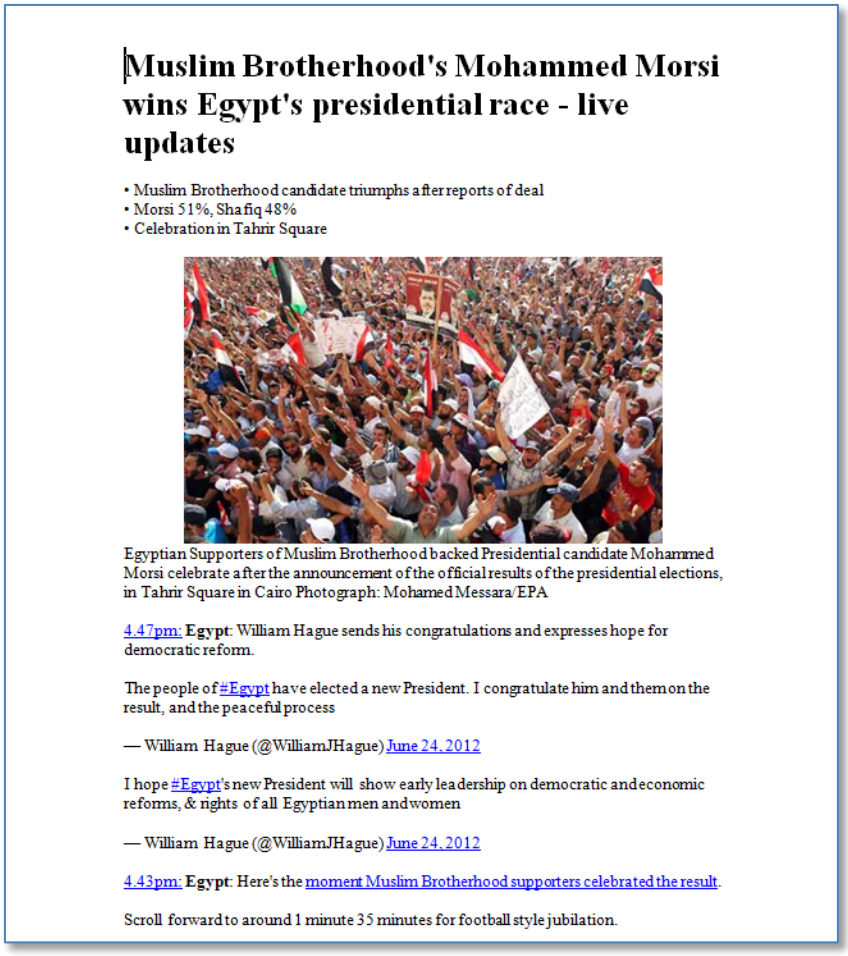
Mitt Romney meets Sunday with Israel's Prime Minister Benjamin Netanyahu in Jerusalem.

Sponsored Links

Romney has said he has a "zero tolerance" policy toward Iran obtaining the capability to build a nuclear weapon.

"If Israel has to take action on its own, in order to stop Iran from developing the capability, the governor would respect that decision," foreign policy adviser Dan Senor told reporters ahead of the speech, planned for late Sunday near Jerusalem's Old City.

Word document, contained in SFX RAR file
C8202523F35295E8BC8CC1731EDB0559



Muslim Brotherhood's Mohammed Morsi wins Egypt's presidential race - live updates

- Muslim Brotherhood candidate triumphs after reports of deal
- Morsi 51%, Shafiq 48%
- Celebration in Tahrir Square

Egyptian Supporters of Muslim Brotherhood backed Presidential candidate Mohammed Morsi celebrate after the announcement of the official results of the presidential elections, in Tahrir Square in Cairo Photograph: Mohamed Messara/EPA

4.47pm: **Egypt**: William Hague sends his congratulations and expresses hope for democratic reform.

The people of #Egypt have elected a new President. I congratulate him and them on the result, and the peaceful process

— William Hague (@WilliamJHague) June 24, 2012

I hope #Egypt's new President will show early leadership on democratic and economic reforms, & rights of all Egyptian men and women

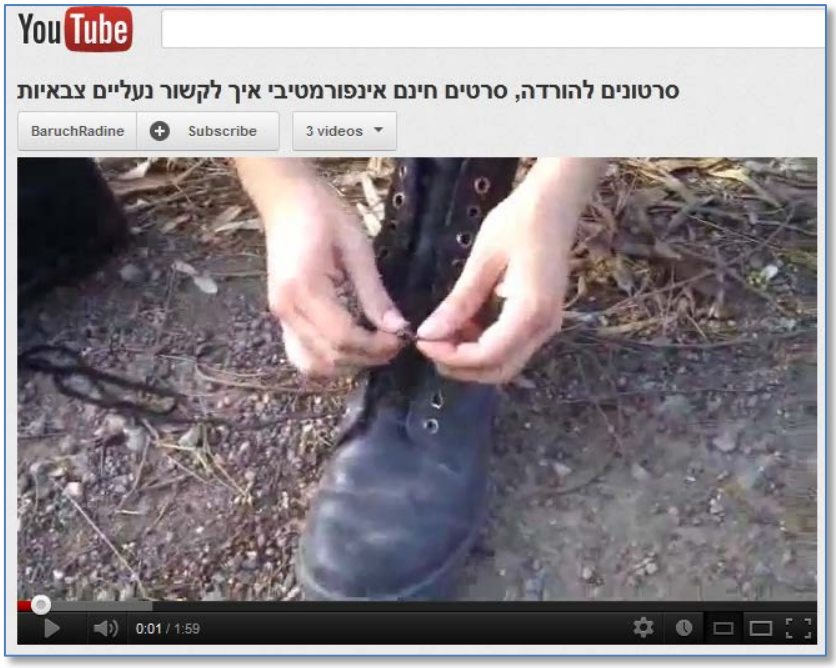
— William Hague (@WilliamJHague) June 24, 2012

4.43pm: **Egypt**: Here's the moment Muslim Brotherhood supporters celebrated the result.

Scroll forward to around 1 minute 35 minutes for football style jubilation.

Word document, contained in SFX RAR file C21D7165B25CAF65D7F92FF758C1B5B1

"The first conference of Dr. Mohamed Morsi, after winning.doc----------.scr"



YouTube URL contained in SFX RAR file 5B740B4623B2D1049C0036A6AAE684B0

"מיילען רושקל ריא יביטמרופניא מניח מיטרס תויאבצ[RTLO]----------.wmv----------.scr"

Found in Israel

The bombed Sudanese factory produced Iranian Shehab missiles

Sudanese missile factory in flames

The Yarmouk Complex of military plants near Khartoum, whicht was bombed five minutes after midnight Wednesday, Oct. 24, by four fighter-bombers, recently went into manufacturing Iranian ballistic surface-to-surface Shehab missiles under license from Tehran, debkafile's military and intelligence sources disclose. Western intelligence sources have not revealed what types of Shehab were being turned out in Sudan but they believe the Yarmouk's output was intended to serve as Tehran's strategic reserve stock in case Iran's ballistic arsenal was hit by Israeli bombers.

The Israeli Air Force has a long record of pre-emptive attacks for destroying an enemy's long-range missiles in the early stages of a conflict. In June 2006, for instance, the IAF destroyed 90 percent of Hizballah's long-range missiles in the first hours of the Lebanon war.

Videos of the explosions caused in the air raid over Sudan showed large quantities of phosphorus flares in the sky suggesting that a large stockpile was demolished along with the manufacturing equipment.

Western sources did not divulge information about the comings and goings of Iranian missile specialists or whether the Bashir government had given Tehran permission to stage attacks from Sudan against Middle East targets, in return for the allotment of a number of missiles to the Sudanese army. All they would say is that the complex's structures had been completely leveled by the aerial bombardment and subsequent fire.

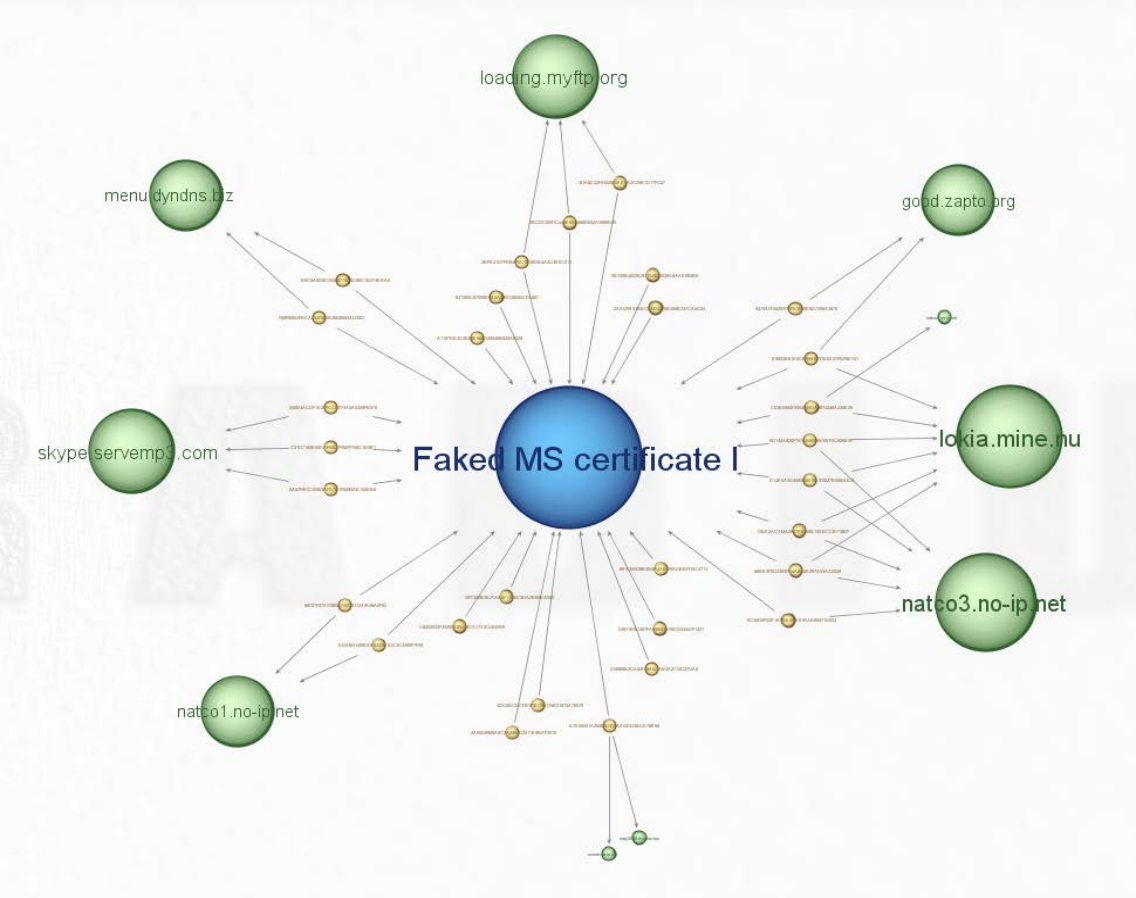
Word document, contained in SFX RAR file 72fd6074915f8f123eb44b3dd475d36b

"TShehab[RTLO]cod.scr"

Found in Israel

Command & Control

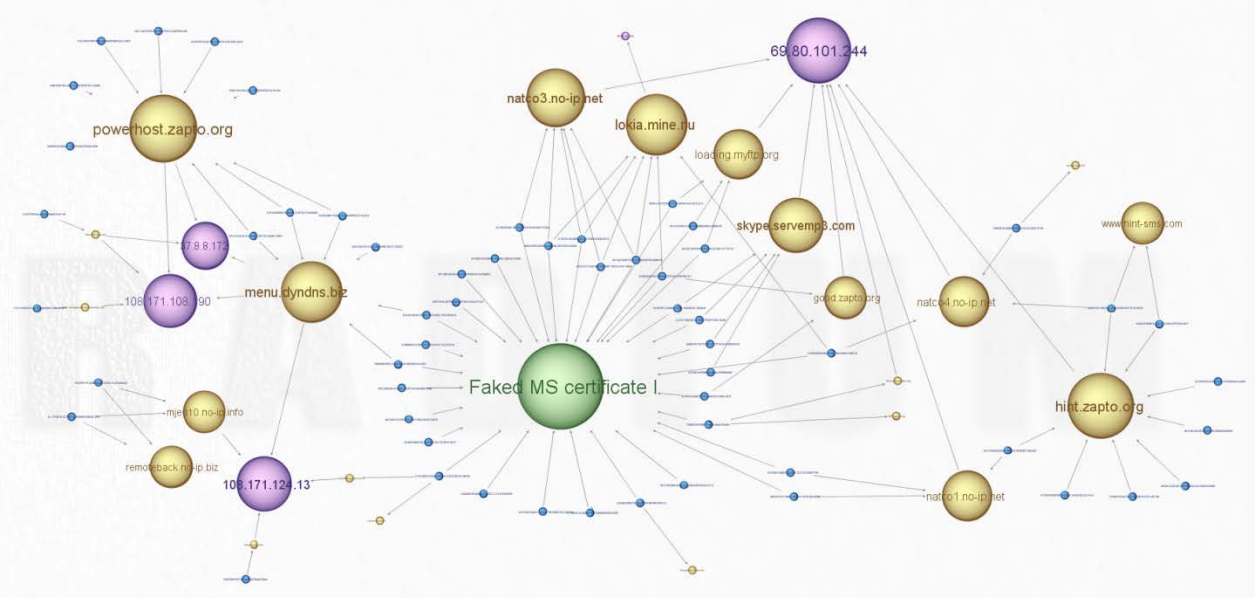
The involved malwares connect to external hosts controlled by the attackers. These belong to various DynDNS services, and at the time of writing resolve to IP addresses located with hosting services in the US.



Samples in yellow connecting to C&C hosts (green). All are digitally signed and connected through the blue certificate node in the middle.

This is where the trail could have ended. However, there are still clues to look at – for example, what *other* executables connect to these C&C hosts. This time, digging into our Malware Analyzer G2 (MAG2) databases shows that there is more malware talking to this infrastructure, and these bots again connect to more C&C domains. These new malwares are also predominantly XtremeRats. However, they have been in circulation for a longer time – *all the way back to October 2011*. I think it is logical to assume that all these have been part of a medium/large surveillance operation.

When updated with this information the plot now looks like this:



Same as previous illustration, where new unsigned samples are shown to be related through the usage of the same C&C infrastructure.Colours have changed – now the certificate is green, the C&C servers are yellow, the samples are blue, while IP addresses are purple. These IP addresses can be considered examples – they change regularly.

Several of these domains appear to be hosted together. For example (at the time of writing):

108.171.108.190 is pointed to by *may2008.dyndns.info, menu.dyndns.biz, flashsoft.no-ip.biz, monagameel.chickenkiller.com, powerhost.zapto.org*
108.171.124.13 is pointed to by *helpme.no-ip.biz, mjed10.no-ip.info*
69.80.101.244 is pointed to by *good.zapto.org, hint.zapto.org, hint1.zapto.org, natco1.no-ip.net, natco2.no-ip.net, natco3.no-ip.net, natco4.no-ip.net, loading.myftp.org, skype.servemp3.com, test.cable-modem.org*

These addresses tend to change. Typically, every couple of days a new IP configuration is introduced for some boxes, while others may remain static – such as the host *lokia.mine.nu,* which has resolved to 69.80.107.129 since we started examining the case.

As mentioned, the IP addresses in use have belonged to mostly US-based hosting services…at least recently.

If we go further back in time (towards spring of 2012) most of the domains used resolved to IP addresses in the range 188.161.*. This range is located in Gaza and belongs to a provider headquartered in Ramallah in the West Bank:

Palestinian Territory, Occupied Gaza Palestine Telecommunications Company (paltel), ASN: AS12975

We have also to a lesser extent seen IP addresses in use belonging to another Paltel division: **Palestinian Territory, Occupied Gaza Hadara Technologies Private Shareholding Company, ASN: AS15975**

What is behind these IP addresses is hard to establish. It is possible that they are hacked boxes, and as such not give much valid information. If that were the case, one might have expected greater IP range and geographical distribution, but nothing is certain.

Our databases also show that there is much more malware talking to these providers through many other DynDNS domains. Some of these are probably also related to this case, but as we have no evidence linking the cases, these malwares have not been included in this paper. It is however interesting to note the hostnames some of these connect to – like "terroristttt.no-ip.biz".

The plot thickens

So far, the impression is of an attack actor attempting to gather information from Israelis. Then something happens that throws this picture in disarray.

A series of samples show up that do not follow the pattern. They apparently do **not** target Israelis. Instead they use Arabic language and refer to Palestinian issues.

مثلما فعلوا بالرئيس الراحل أبو عمار

الموساد يهدد بتصفية الرئيس أبو مازن ما لم يتراجع عن المصالحة مع حماس

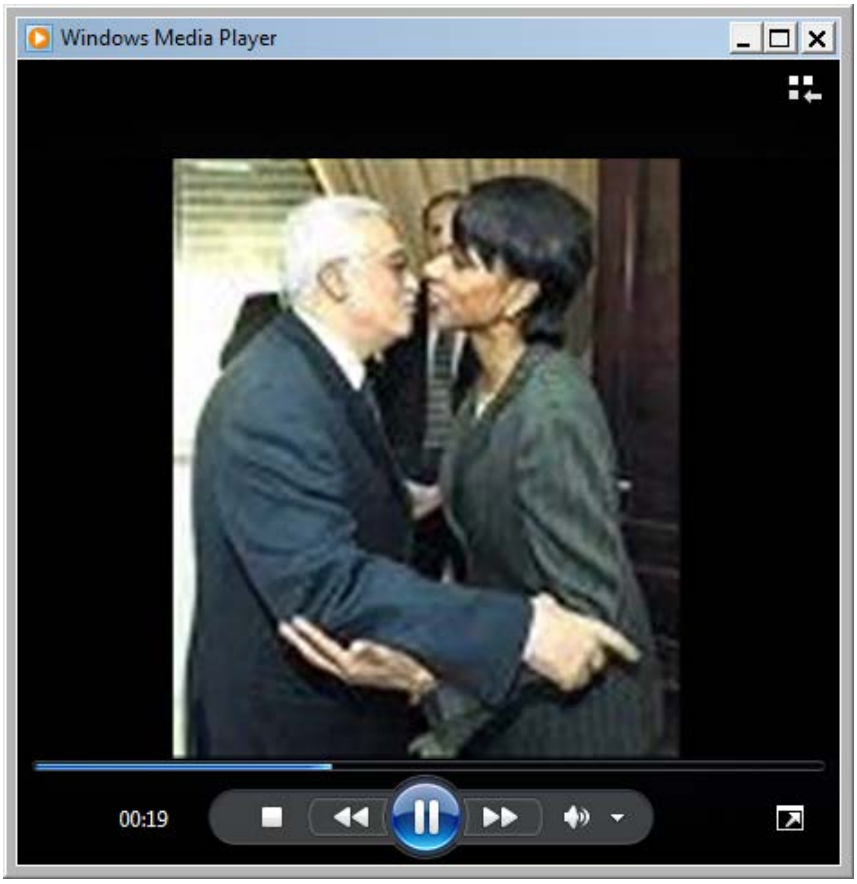
قالت مصادر بالجامعة العربية لشبكة الإعلام العربية في مصر 'محيط' ،إن الرئيس محمود عباس أبو مازن ، تلقي تهديدات من عناصر تابعة لموساد بأن مصيره سيكون مثل مصير أبو عمار إذا ما استمر ،(يتحدي السياسات الإسرائيلية) ، و لا يخضع للاملاءات التي ترده من واشنطن ،وتتعلق بعملية التسوية والسياسة الفلسطينية ، وأوضحت المصادر الإسرائيلية إن تل ابيب أوضحت موقفها للعديد من الدول الإقليمية ودول العالم مؤكدة أن التطورات في المنطقة تحتم عليها اتخاذ إجراءات فاعلة لحفظ أمنها .

واتهمت مصادر أمنية إسرائيلية الرئيس محمود عباس بأنه تجاوز كافة الخطوط الحمراء في اتفاقه الأخير مع حركة حماس بالقاهرة. ونقلت إذاعة جيش الاحتلال عن تلك المصادر قولها إن الرئيس عباس أدار ظهره لعملية السلام بإصراره على التوحد مع حركة حماس معربة عن أملها في أن تتفهم القيادة الفلسطينية وعناصر الاعتدال فيها إن الرئيس عباس يدفع بالمنطقة إلى الهاوية عبر محاولاته التساوق مع اندفاع المنطقة نحو التطرف وان تقوم بما يلزم لايقافه

وقالت المصادر ان اسرائيل لن تسمح لعباس بتشكيل جبهة مع المتطرفين الفلسطينيين والعرب في الوقت الذي يزداد فيه تسلح فصائل غزة والتي باتت تشكل تهديدا استراتيجا للدولة العبرية.

Word document contained in EXE file
FC17F3B2E2C7F5F24D35899D95B8C4A6

This document in Arabic claims that Mahmoud Abbas is threatened by assassination by Mossad if he does not stop his reconciliation policy towards Hamas. The image is taken from a news story about Abbas speaking at a meeting in Ramallah.



The sample containing this video is digitally signed in the same way as the initial samples, but the baiting angle is different. Instead of showing information interesting for an Israeli audience, the video contains a music piece critical of Mahmoud Abbas, claiming that he is not working for the good of the Palestinian people.

الأســـرار الخفيـــة وراء صفقة تبادل الأســـرى مع الجعبـــري والضابط الاســـرائيلي فيلدان

זטכ"יל
קסאם

اعلن مصدر رفيع المستوى في حركة حماس ان صفقة تبادل الاسرى مع اسرائيل "قد انجزت برعاية مصرية وان التنفيذ سيكون بداية الشهر المقبل "نوفمبر.

واضاف المصدر ان خالد مشعل رئيس المكتب السياسي لحركة حماس سيخرج في مؤتمر صحفي خلال ساعات لتوضيح الاتفاق.

وفي التفاصيل فان الصفقة التي اشرف عليها وزير المخابرات المصرية مراد موافي شخصيا في مقر المخابرات المصرية قبل اسبوعين بحضور وفدي حماس برئاسة احمد الجعبري، واسرائيل فان الصفقة تتضمن الافراج عن الف اسير مقابل شاليط سيتم الافراج عن 450 اسير قبلا الافراج عنه و550 بعد الافراج عنه وان الاسيرات جميعهن مشمولات في الصفقة فيما لم يعرف حتى الان اسماء الاسرى المفرج عنهم والذين سيعلن عنهم خالد مشعل في مؤتمر صحفي بعد ساعات

بدورها وخلال انعقاد جلستها اقرت الحكومة الاسرائيلية الليلة صفقة التبادل وقالت انها ستعطي 48 ساعة لبعض الاشخاص للاعتراض على بعض الاسماء المفرج عنهم امام المحكمة، وسيتم تنفيذ الصفقة بعد يوم الاحد.

Word document contained in SFX ZIP file
B4F5BFC0AB0CC3D6B7A6B9653784DE56

Found in Palestine

This document revolves around the prisoner exchange deal with the Israeli government over the Israeli soldier Gilad Shalit, held hostage by Hamas for over five years.

JPEG image contained in EXE file
0AA7B256D2DCC8BD3914F895B134B225

This image appears purportedly to be of Gilad Shalit in his hostage cell. This could be aimed at Israelis, but the image itself has been mostly shown on Arabic/Palestinian sites like *www.shehab.ps*, a news agency located in Gaza.

فاليم فتح طالبت في مذكرة للرئيس بعقد مؤتمر استثنائي لترتيب الوضع الداخلي للحركة.. واذا استمر الوضع الحالي سيتكرر فشل الانتخابات

حذر نبيل عمرو عضو المجلس الاستشاري لحركة فتح السفير الفلسطيني السابق من تكرار تجربة الانتخابات 'بالقاهرة الأربعاء في حديث مطول مع 'القدس العربي التشريعية الفلسطينية التي جرت عام 2006 وفازت بها حركة حماس جراء الفرقة التي كانت سائدة في صفوف حركة فتح، مطالبا بالعمل بشكل جاد لتوحيد صفوف الحركة، وتعزيز مكانتها بالشارع الفلسطيني استعدادا للانتخابات التشريعية والرئاسية المقررة في ايار (مايو) المقبل وفق اتفاق المصالحة الذي وقع في القاهرة قبل شهور.

واضاف عمرو الذي شارك في دورة اجتماعات المجلس الاستشاري لحركة فتح التي عقدت الاسبوع الماضي بحضور الرئيس محمود عباس قائلا للقدس العربي الاربعاء 'نعم هنالك قلق واذا استمر الوضع في فتح على حاله فان ماحدث في الماضي من فشل على صعيد الانتخابات المحلية والنقابية والتشريعية سوف يتكرر'.

وفيما يلي الحوار الذي اجرته 'القدس العربي' مع عمرو حول اوضاع حركة فتح في ظل الاستعدادات الجارية للانتخابات في ايار المقبل وما تشهده الساحة السياسية الفلسطينية.

استاذ نبيل عمرو عضو المجلس الاستشاري لحركة فتح لماذا طالبتم في بيان - اصدره المجلس مؤخرا عقب اجتماعه الاسبوع الماضي برئاسة الرئيس محمود عباس بضرورة عقد مؤتمر استثنائي للحركة قبل اجراء الانتخابات الرئاسية والتشريعية في ايار المقبل ؟

Word document contained in EXE file
926235FCF7B91442A405B5760A0729EB

This document is an interview with the former Palestinian ambassador and Member of Parliament Nabil Amr. He is known to have been critical of Arafat and later Abbas.

We also see attacks apparently against Palestinian targets without being able to tie them up against the already mentioned attack/C&C structure. For example, a file received by us as “d.exe”, (MD5 1f1e9958440d773c34415d9eb6334b25), found in Palestine Nov 17th last year, shows a PDF document with content seemingly taken from “Palestine Now” (www.paltimes.net):

PDF document contained in the EXE file 1F1E9958440D773C34415D9EB6334B25

Found in Palestine

Document metadata

Most of the bait attachments are Word documents, and Word documents can contain metadata (typically the usernames of the creator and the one who last saved the document). It is possible to scrub these details, but our attackers seem to have forgotten this – or inserted faked data.

Palestinian baits:

Hmas.doc:	*Created by "Hitham", saved by "anar"*	*date Oct 12th 2011*
484hhh.doc:	*Created by "Hitham", saved by "Ayman"*	*date Nov 27th 2011*
Word.doc:	*Created and saved by "Tohan"*	*date Feb 18th 2012*

Israeli baits:

word.doc:	*Created by "ahmed", saved by "aert"*	*date May 14th 2012*
IDF NEWS.doc:	*Created and saved by "aert"*	*date May 26th 2012*
Brotherhood.doc:	*Created and saved by "aert"*	*date Jun 24th 2012*
detl.doc:	*Created and saved by "aert"*	*date Jun 29th 2012*
Advisor.doc:	*Created and saved by "HinT"*	*date Jul 29th 2012*
IDF.doc:	*Created and saved by "aert"*	*date Aug 1st 2012*
System.doc:	*Created and saved by "HinT"*	*date Aug 5th 2012*
York.doc:	*Created and saved by "HinT"*	*date Oct 16th 2012*
barrage.doc :	*Created and saved by "HinT"*	*date Oct 24th 2012*
shehab.doc:	*Created and saved by "HinT"*	*date Oct 31st 2012*

There seems to be a number of people involved in creating these bait files. The dates also roughly coincide with the apparent shift in IP ranges (Appendix B), from first being located in Gaza, to being located internationally.

Conclusion

We have uncovered a substantial number of malware executables that contain information seemingly tailored at Israelis and Palestinians. We have the impression that a cybersurveillance operation is underway (and is probably still ongoing - most recent sample created Oct. 31) which was first mainly focused on Palestinian targets, then shifted towards Israel. The reason for the shift is unknown. Maybe it was planned all along; or caused by changes in the political climate; or maybe the first half of the operation found data that caused the target change.

This analysis is almost exclusively based on the executable files themselves. We have very little information about actual infections. The only documented case is the Benny Gantz-themed email which triggered the investigation. We consider it likely that other attacks have been modeled the same way, using attachments in email. These attachments may often have consisted of the described malicious files inside archives like RAR or ZIP.

The attacker is still unknown to us. There are probably several actors that could have an interest in the regional politics, as the various powerblocks in the region are manifold and conflicted. By using largely off-the-shelf malware, the cost of mounting such an operation is considerably lower than for those who do their own malware development.

References

1. **Ravid, Barak.** Haaretz.com: Israel's Foreign Ministry targeted by computer virus bearing IDF chief's name. [Online] http://www.haaretz.com/blogs/diplomania/israel-s-foreign-ministry-targeted-by-computer-virus-bearing-idf-chief-s-name.premium-1.472278.

Appendix A: C&C hostnames

may2008.dyndns.info
menu.dyndns.biz
flashsoft.no-ip.biz
monagameel.chickenkiller.com
hatamaya.chickenkiller.com
powerhost.zapto.org
helpme.no-ip.biz
mjed10.no-ip.info
good.zapto.org
hint.zapto.org
hint1.zapto.org
natco1.no-ip.net
natco2.no-ip.net
natco3.no-ip.net
natco4.no-ip.net
loading.myftp.org
skype.servemp3.com
test.cable-modem.org
idf.blogsite.org
javaupdate.no-ip.info
lokia.mine.nu
www.hint-sms.com
owner.no-ip.biz
remoteback.no-ip.biz
ramadi.no-ip.biz

The likelihood that there are more names involved is large. There is for example a domain natco5.no-ip.net which resolves to the same IP's as the rest of the series, but we have not seen the malware which uses it – yet.

Appendix B: C&C Timeline

MD5	Primary C&C	C&C loc.	Date first seen
A5DE87646EE943CD1F448A67FDBE2817	hint.zapto.org	PS	27-Oct-11
F982401E46864F640BCAEDC200319109	natco4.no-ip.net	PS	29-Oct-11
EC5B360F5FF6251A08A14A2E95C4CAA4	hint1.zapto.org	PS	02-Nov-11
97576FA7A236679DBE3ABE1A4E852026	mjed10.no-ip.info	PS	07-Nov-11
C1EC435E97A4A4C5585392D738B5879F	monagameel.chickenkiller.com	PS	07-Nov-11
2559FE4EB88561138CE292DF5D0E099F	powerhost.zapto.org	PS	08-Nov-11
0ABF3FA976372CBC8BF33162795E42A8	powerhost.zapto.org	PS	14-Nov-11
0B3B1E2E22C548D8F53C2AA338ABD66E	hint.zapto.org	PS	19-Nov-11
0AA7B256D2DCC8BD3914F895B134B225	hint.zapto.org	PS	30-Nov-11
FF8E19CA8A224CC843BF0F2F74A3274E	powerhost.zapto.org	PS	17-Dec-11
7C5272F3F24ACB225270DDED72CFC1D4	flashsoft.no-ip.biz	PS	23-Dec-11
8AEAA0C81A36449EC9613CA846E196F2	menu.dyndns.biz	PS	01-Jan-12
2AAD951DBECB6D4715B306B337CA5C34	mjed10.no-ip.info	PS	03-Jan-12
926235FCF7B91442A405B5760A0729EB	helpme.no-ip.biz	PS	12-May-12
963BFAE19B3DA5BECE081DFF1D1E3EF9	hint.zapto.org	US	16-May-12
EBC9BDF9FDF0A9773899D96D24AC46F4	powerhost.zapto.org	PS	19-May-12
998F30457BC48A1A6567203E0EC3282E	powerhost.zapto.org	PS	29-May-12
31F96ADD841594D35E6E97376114E756	hint.zapto.org	FR	02-Jun-12
6E416C45A833F959A63785892042595A	hint.zapto.org	PS	02-Jun-12
0DC102CFB87C937EEFFE01A06F94E229	powerhost.zapto.org	PS	07-Jun-12
B7DF947B4A67A884C751840F83C4405E	hint.zapto.org	UK	09-Jun-12
2EB1503751A7C74890096B1837C7BD81	menu.dyndns.biz	PS	09-Jun-12
C21D7165B25CAF65D7F92FF758C1B5B1	skype.servemp3.com	US	25-Jun-12
0A67F9CC30083AFB7E1F8295AE152BB6	skype.servemp3.com	US	25-Jun-12
E9823B61E6CE999387DE821DFBF6E741	good.zapto.org	US	10-Jul-12
2AAD951DBECB6D4715B306B337CA5C34	good.zapto.org	US	12-Jul-12
ED53831468DDF4220E1DC3C3398F7F39	natco1.no-ip.net	US	02-Aug-12
66DDF27517985A75B2317231B46A6F62	natco1.no-ip.net	US	02-Aug-12
86BE5F0D2303FB4A8A8E297A53AC0026	lokia.mine.nu	US	14-Aug-12
D14E0A3D408065B1551F2827B50B83CA	lokia.mine.nu	US	29-Aug-12
B6C8A6D6C35428779C5C65C1B273EBA0	menu.dyndns.biz	US	04-Sep-12
C03B5985F2504939DA9874246A439E25	lokia.mine.nu	US	10-Sep-12
216689B2CA82F16A0CAB3A2712C27DA6	natco2.no-ip.net	US	18-Sep-12
9C39D6F52E1E1BE5AE61BAB90971D054	natco3.no-ip.net	US	27-Sep-12
E7E05001A294EBFE8A012DD3BCE78E96	may2008.dyndns.biz	US	28-Sep-12
F68F85B0FBCA450F0D5C8828063AD30D	menu.dyndns.biz	US	02-Oct-12
3DA8C22F5340850EE5A2C25B1D17FC27	loading.myftp.org	US	03-Oct-12
9D144A828F757A90B86976EF0C906B3F	lokia.mine.nu	US	21-Oct-12
DBE2AC744A3947B6306E13EBCCB718BF	lokia.mine.nu	US	21-Oct-12
861C90536B3B5A4A8309ADBBFD5C4713	natco3.no-ip.net	US	24-Oct-12
947557A55267DFFB3F85E0D7496A3679	good.zapto.org	US	25-Oct-12
2BFE41D7FDB6F4C1E38DB4A5C3EB1211	loading.myftp.org	US	25-Oct-12
2BCDC5091C446E8B6888D802A3589E09	loading.myftp.org	US	25-Oct-12
72FD6074915F8F123EB44B3DD475D36B	idf.blogsite.org	US	31-Oct-12
41454B390B73A45004B916B96C693312	javaupdate.no-ip.info	US	03-Nov-12

Red hash = probable PS target. Blue hash = probable IL target.

Appendix C: MD5 list, main cluster

MD5
A5DE87646EE943CD1F448A67FDBE2817
F982401E46864F640BCAEDC200319109
EC5B360F5FF6251A08A14A2E95C4CAA4
97576FA7A236679DBE3ABE1A4E852026
C1EC435E97A4A4C5585392D738B5879F
2559FE4EB88561138CE292DF5D0E099F
0ABF3FA976372CBC8BF33162795E42A8
1f1e9958440d773c34415d9eb6334b25
0B3B1E2E22C548D8F53C2AA338ABD66E
0AA7B256D2DCC8BD3914F895B134B225
B455426811B82CB412952F63D911D2A8
E431634699D7E5025ECDF7B51A800620
FF8E19CA8A224CC843BF0F2F74A3274E
7C5272F3F24ACB225270DDED72CFC1D4
8AEAA0C81A36449EC9613CA846E196F2
FC17F3B2E2C7F5F24D35899D95B8C4A6
926235FCF7B91442A405B5760A0729EB
963BFAE19B3DA5BECE081DFF1D1E3EF9
EBC9BDF9FDF0A9773899D96D24AC46F4
4A06D9989A8C3A9967C2011E5BAF3010
4DC0BCDCFB3F3D794175B21872A76079
998F30457BC48A1A6567203E0EC3282E
91FC9D1B635FDEE4E56AEC32688A0E6C
940B3ACDF1E26FCCCF74A5A0359FB079
cebc8b51d51e442e2af8c86e70c8adf4
31F96ADD841594D35E6E97376114E756
6E416C45A833F959A63785892042595A
0DC102CFB87C937EEFFE01A06F94E229
B7DF947B4A67A884C751840F83C4405E
2EB1503751A7C74890096B1837C7BD81
C21D7165B25CAF65D7F92FF758C1B5B1
0A67F9CC30083AFB7E1F8295AE152BB6
15FC009D9CAAA8F11D6C3DA2B69EA06E
D9D1B0C467FA4999DEF6CD53447F1221
E9823B61E6CE999387DE821DFBF6E741
2AAD951DBECB6D4715B306B337CA5C34
ED53831468DDF4220E1DC3C3398F7F39
66DDF27517985A75B2317231B46A6F62
86BE5F0D2303FB4A8A8E297A53AC0026
A1187DE4C4B88E560D46940B820A6228
D14E0A3D408065B1551F2827B50B83CA
B6C8A6D6C35428779C5C65C1B273EBA0
841565C67006E6A0A450C48054CF348C
C8202523F35295E8BC8CC1731EDB0559
C03B5985F2504939DA9874246A439E25
216689B2CA82F16A0CAB3A2712C27DA6
5B740B4623B2D1049C0036A6AAE684B0
9C39D6F52E1E1BE5AE61BAB90971D054
E7E05001A294EBFE8A012DD3BCE78E96
F68F85B0FBCA450F0D5C8828063AD30D
3DA8C22F5340850EE5A2C25B1D17FC27
9D144A828F757A90B86976EF0C906B3F
DBE2AC744A3947B6306E13EBCCB718BF
861C90536B3B5A4A8309ADBBFD5C4713
947557A55267DFFB3F85E0D7496A3679
2BFE41D7FDB6F4C1E38DB4A5C3EB1211
2BCDC5091C446E8B6888D802A3589E09
72FD6074915F8F123EB44B3DD475D36B
41454B390B73A45004B916B96C693312